CLAIMS

1. A data division method for dividing original data into as many divided data as a desired number of division by using a prescribed processing unit bit length, comprising the steps of:

generating a plurality of original partial data by dividing the original data by the prescribed processing unit bit length;

generating a plurality of random number partial data each having a length equal to the prescribed processing unit bit length, from a random number having a length less than or equal to a bit length of the original data, in correspondence to the plurality of original partial data;

generating a plurality of divided partial data that constitute each divided data by using exclusive OR calculation of the original partial data and the random number partial data, each divided partial data having a length equal to the prescribed processing unit bit length; and

generating the divided data in the desired number of division from the plurality of divided partial data, such that the original data cannot be ascertained from any one divided data alone but the original data can be recovered from a prescribed number of the divided data among generated divided data.

2. The data division method of claim 1, wherein the original partial data and the random number partial data are generated as many as the desired number of division minus one.

3. The data division method of claim 1, wherein the divided data include one or more divided data formed by a random number alone, and one or more divided data formed by

the divided partial data generated by the exclusive OR calculation of one or more original partial data and one or more random number partial data.

4. The data division method of claim 3, wherein the one divided data formed by a random number alone is formed by repeating a random number with an arbitrarily determined length.

5. The data division method of claim 3, wherein the one divided data formed by a random number alone is formed by a pseudo-random number generated from information of a prescribed length according to a pseudo-random number generation algorithm.

6. The data division method of claim 1, wherein the divided data include two or more divided data formed by the divided partial data generated by the exclusive OR calculation of one or more original partial data and one or more random number partial data.

7. The data division method of claim 1, wherein when the original data, the random number, the divided data, the desired number of division and the processing unit bit length are denoted as S, R, D, n and b, respectively, variables i (= 1 to n) and j (= 1 to n-1) are used as variables, each one of (n-1) sets of the original partial data, (n-1) sets of the random number partial data, n sets of the divided data D, and (n-1) sets of divided partial data of each divided data are denoted as S(j), R(j), D(j), and D(i,j), respectively, each original partial data S(j) is generated as b bits of data from b×(j-1)+1-th bit of the original data S while changing a variable j from 1 to n-1, U[n,n] is an n×n matrix with u(i,j) indicating a value of i-th row and j-th column given by:

$u(i,j) = 1$ when $i+j \leq n+1$
$u(i,j) = 0$ when $i+j > n+1$

P[n,n] is an n×n matrix with p(i,j) indicating a value of i-th row and j-th column given by:

$p(i,j) = 1$ when $j = i+1$
$p(i,j) = 1$ when $i = 1,\ j = n$
$p(i,j) = 0$ otherwise

c(j,i,k) is defined as a value of i-th row and k-th column of an (n-1)×(n-1) matrix U[n-1,n-1]×P[n-1,n-1]ˆ(j-1), where U[n-1,n-1]×P[n-1,n-1]ˆ(j-1) denotes a product of a matrix U[n-1,n-1] and (j-1) sets of a matrix ×P[n-1,n-1], and Q(j,i,k) is defined as Q(j,i,k) = R(k) when c(j,i,k) = 1 and Q(j,i,k) = 0 when c(j,i,k) = 0,

each divided partial data D(i,j) is generated by:

$D(i,j) = S(j)*(\prod_{k=1}^{n-1} Q(j,i,k))$ when $i < n$

$D(i,j) = R(j)$ when $i = n$

while changing a variable i from 1 to n and changing a variable j from 1 to n-1 for each variable i, where

$$\prod_{k=1}^{n-1} Q(j,i,k) = Q(j,i,1)*Q(j,i,2)* \cdots *Q(j,i,n-1)$$

and * denotes the exclusive OR calculation.

8. The data division method of claim 1, wherein each divided data is generated such that a random number component cannot be eliminated by carrying out calculation among the divided partial data that constitute the each divided data.

9. The data division method of claim 8, wherein each divided data is generated by first generating the plurality of divided partial data that constitute each divided data by using a prescribed definition formula formed by the exclusive OR calculation of the original partial data and the random number partial data, and then interchanging one divided partial data and another divided partial data among the divided partial data that constitute each divided data.

10. The data division method of claim 8, wherein each divided data is generated by first generating the plurality of divided partial data D(i,j) that constitute each divided data D(i) by using a prescribed definition formula formed by the exclusive OR calculation of the original partial data and the random number partial data, and then removing a j-th random number partial data R(j) from D(i,j) with a value of i in a range of n-1 > i > 0, where n is the desired number of division, j = (n-1)×m+1, and m ≥ 0 is an arbitrary integer.

11. A data division device for dividing original data into as many divided data as a desired number of division by using a prescribed processing unit bit length, comprising:

an original partial data generation unit configured to generate a plurality of original partial data by dividing the original data by the prescribed processing unit bit length;

a random number generation unit configured to generate a plurality of random number partial data each having a length equal to the prescribed processing unit bit length, from a random number having a length less than or equal to a bit length of the original data, in correspondence to the plurality of original partial data;

a divided partial data generation unit configured to generate a plurality of divided partial data that constitute each divided data by using exclusive OR calculation of the original partial data and the random number partial data, each divided partial data having a length equal to the prescribed processing unit bit length; and

a divided data generation unit configured to generate the divided data in the desired number of division from the plurality of divided partial data, such that the original data cannot be ascertained from any one divided data alone but the original data can be recovered from a prescribed number of the divided data among generated divided data.

12. A computer program product for causing a computer to function as a data division device for dividing original data into as many divided data as a desired number of division by using a prescribed processing unit bit length, the computer program product comprising:

a first computer program code for causing the computer to generate a plurality of original partial data by dividing the original data by the prescribed processing unit bit length;

a second computer program code for causing the computer to generate a plurality of random number partial data each having a length equal to the prescribed processing unit bit length, from a random number having a length less than or equal to a bit length of the original data,in correspondence to the plurality of original partial data;

a third computer program code for causing the computer to generate a plurality of divided partial data that constitute each divided data by using exclusive OR calculation of the original partial data and the random number partial data, each divided partial data having a length equal to the prescribed processing unit bit length;

and

a fourth computer program code for causing the computer to generate the divided data in the desired number of division from the plurality of divided partial data, such that the original data cannot be ascertained from any one divided data alone but the original data can be recovered from a prescribed number of the divided data among generated divided data.